

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-215284

(43) 公開日 平成10年(1998) 8月11日

(51) Int. Cl. ⁶	識別記号	F I		
H04L 12/66		H04L 11/20		B
G06F 15/00	330	G06F 15/00	330	B
G09C 1/00	660	G09C 1/00	660	E
H04L 9/32		H04M 3/00		B
H04M 3/00		H04L 9/00	673	C

審査請求 未請求 請求項の数 8 O L (全14頁) 最終頁に続く

(21) 出願番号 特願平9-15147

(22) 出願日 平成9年(1997) 1月29日

(71) 出願人 597013076

株式会社アド・ホック

北海道札幌市中央区南2条西7丁目6-2

日宝南2条ビル5階

(72) 発明者 澤田 原

北海道札幌市中央区南2条西7丁目6-2

日宝南2条ビル5階 株式会社アド・ホック内

(72) 発明者 曾田 亮

北海道札幌市中央区南2条西7丁目6-2

日宝南2条ビル5階 株式会社アド・ホック内

(74) 代理人 弁理士 木内 光春

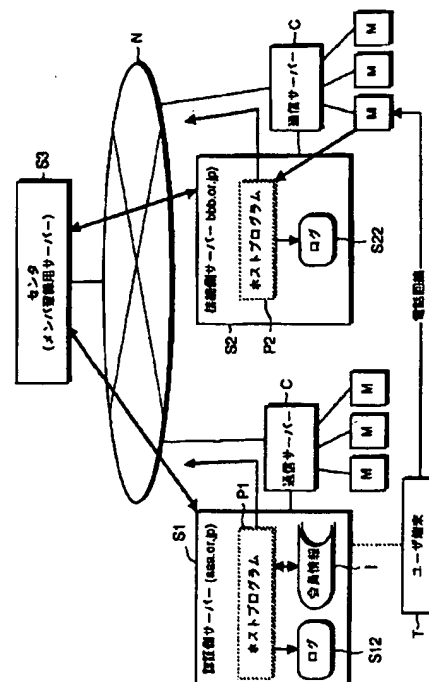
最終頁に続く

(54) 【発明の名称】 ネットワーク接続システム及びネットワーク接続方法

(57) 【要約】

【課題】 複数のサーバー間で会員情報及び接続回線設備を相互利用することによって、接続性に優れたネットワーク接続システムを提供する。

【解決手段】 ユーザーは、自己の会員情報を保有する認証側サーバーS1が混雑しているときや地理的に遠い場合、他のサーバーである接続側サーバーS2にユーザIDとパスワードを送信することによって接続要求を行う。ユーザが送信したユーザIDとパスワードは、接続側サーバーS2から認証側サーバーS1に転送され、認証側サーバーS1で会員情報と照合することによってユーザ認証が行われる。接続側サーバーS2では、ユーザ認証の結果を受けてログイン処理が行われるので、ユーザはインターネット接続サービスを利用することができる。



【特許請求の範囲】

【請求項 1】 ネットワークへの接続回線設備を備えた複数のサーバーを有し、

前記サーバーは、
ユーザに関する会員情報を有する認証側サーバーと、
前記認証側サーバーと所定の関係を有する接続側サーバーを含み、

前記接続側サーバーは、ユーザから送信されるユーザ ID 及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に

10 応じてユーザに提供する接続手段を有し、
前記認証側サーバーは、前記接続側サーバーから送信されるユーザ ID 及びパスワードを前記会員情報と照合することによってユーザ認証を行うユーザ認証手段を有することを特徴とするネットワーク接続システム。

【請求項 2】 前記接続側サーバー及び認証側サーバーはそれぞれ、前記ネットワークへの接続の開始及び終了に関する所定の情報を送受信することによって、接続ログを記録する記録手段を有することを特徴とする請求項 1 記載のネットワーク接続システム。

【請求項 3】 前記接続側サーバーの前記記録手段及び前記認証側サーバーの前記記録手段は、前記接続の開始から終了に至る間、所定の間隔で所定の情報を送受信することによって前記接続が継続しているか否かを確認するように構成されたことを特徴とする請求項 2 記載のネットワーク接続システム。

【請求項 4】 相互に所定の関係を有する複数のサーバーをメンバとして登録する登録手段と、
任意のサーバーがメンバであるか否かの問い合わせに
20 応答するサーバー認証手段と、
を有するメンバ登録用サーバーを備えたことを特徴とする請求項 1、2 又は 3 記載のネットワーク接続システム。

【請求項 5】 前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーが、
前記ユーザ認証のために授受する情報を暗号化し及び復号するための暗号管理手段を有することを特徴とする請求項 1、2、3 又は 4 記載のネットワーク接続システム。

【請求項 6】 ネットワークへの接続回線設備を備えた
40 複数のサーバーを用い、

前記サーバーは、
ユーザに関する会員情報を有する認証側サーバーと、
前記認証側サーバーと所定の関係を有する接続側サーバーを含むネットワーク接続システムにおいて、

前記接続側サーバーは、ユーザから送信されるユーザ ID 及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に
50 応じてユーザに提供し、
前記認証側サーバーは、前記接続側サーバーから送信さ

れるユーザ ID 及びパスワードを前記会員情報と照合することによってユーザ認証を行うことを特徴とするネットワーク接続方法。

【請求項 7】 前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーは、
前記ユーザ認証のために授受する情報を暗号化し及び復号するための処理を実行することを特徴とする請求項 6 記載のネットワーク接続方法。

【請求項 8】 ネットワークへの接続サービスをユーザ端末から受け付ける接続側サーバーと、ユーザに関する会員情報に基づいてユーザ認証を行う認証側サーバーと、を用いたネットワーク接続方法において、
ユーザ端末と認証側サーバーとの間で、ユーザ ID 及びパスワードの授受を、前記接続側サーバーを経由して暗号を用いて行うために、

認証側サーバーが、一時的公開鍵 T-Pk を固有の秘密鍵 F-Sk で暗号化することによって第 1 の暗号データを作成するステップと、

20 認証側サーバーが、作成した前記第 1 の暗号データをユーザ端末に送信するステップと、

ユーザ端末が、送信された前記第 1 の暗号データから、前記固有の秘密鍵 F-Sk に対応する公開鍵 F-Pk を用いて前記一時的公開鍵 T-Pk を復号するステップと、

ユーザ端末が、復号した前記一時的公開鍵 T-Pk を用いて、ユーザ ID 及びパスワードを暗号化することによって第 2 の暗号データを作成するステップと、

ユーザ端末が、作成した前記第 2 の暗号データを認証側サーバーに送信するステップと、

30 認証側サーバーが、送信された前記第 2 の暗号データから、前記一時的公開鍵 T-Pk に対応する一時的秘密鍵 T-Sk を用いてユーザ ID 及びパスワードを復号するステップと、

を含むことを特徴とするネットワーク接続方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ユーザ端末をインターネットなどの広域ネットワークに接続するためのネットワーク接続システム及びネットワーク接続方法の改良に関するもので、特に、接続サービスを提供する複数のサーバー間で、会員情報及び接続回線設備を相互利用することによって、接続性に優れたネットワーク接続システム及びネットワーク接続方法を提供するものである。

【0002】

【従来の技術】近年、国際的な情報通信ネットワークとして、インターネットが急速に普及し、その重要性が増大しつつある。インターネットを利用する場合、一般のユーザは、インターネット接続業者（ISP：インターネットサービスプロバイダ）と契約し、電話回線とモデ

ムを介してプロバイダのサーバーにログインし、サーバーを通じてインターネット上の情報にアクセスする。

【0003】

【発明が解決しようとする課題】従来では、異なる複数のプロバイダのサーバー間で、会員情報及び回線接続設備を相互利用する手段は存在しなかったため、会員が接続できるのは契約先のプロバイダ（加入プロバイダ）のサーバーに限定されていた。このため、回線が混雑して加入プロバイダのサーバーに接続できない場合でも、他のプロバイダのサーバーを介してインターネットに接続することはできなかった。この結果、加入プロバイダの回線混雑時に接続性が低下するという不都合が生じていた。また、電話回線使用料の観点から、ユーザもプロバイダも地理的に近い相手を契約対象として選ばざるを得なかった。このことは、ユーザによるプロバイダ選択の自由を狭めると共に、プロバイダによる新規会員募集の範囲も限定し、インターネットの普及を妨げていた。

【0004】本発明は、上記のような従来技術の問題点を解決するために提案されたもので、その目的は、複数のサーバー間で会員情報及び接続回線設備を相互利用することによって、接続性に優れたネットワーク接続システム及びネットワーク接続方法を提供することである。また、本発明の他の目的は、会員情報を保有するサーバーと実際の接続を行うサーバーとの間で、接続に関する所定の情報を送受信することによって、双方で正副の同一内容の接続ログを記録し、接続ログの信頼性に優れたネットワーク接続システムを提供することである。

【0005】また、本発明の他の目的は、ログイン時に接続側サーバーを経由するパスワードなどを暗号化することによって、セキュリティの優れたネットワーク接続システム及びネットワーク接続方法を提供することである。また、本発明の他の目的は、相互に所定の関係を有するサーバーの情報を、単一のメンバ登録用サーバーに登録し、メンバからの照会に回答することによって、信頼性とセキュリティに優れたネットワーク接続システムを提供することである。また、本発明の他の目的は、接続側と認証側のサーバー間で接続の継続を確認することによって、接続ログに記録される内容の信頼性が高いネットワーク接続システムを提供することである。

【0006】

【課題を解決するための手段】上記の目的を達成するため、請求項1のネットワーク接続システムは、ネットワークへの接続回線設備を備えた複数のサーバーを有し、前記サーバーは、ユーザに関する会員情報を有する認証側サーバーと、前記認証側サーバーと所定の関係を有する接続側サーバーを含み、前記接続側サーバーは、ユーザから送信されるユーザID及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に応じてユーザに提供する接続

手段を有し、前記認証側サーバーは、前記接続側サーバーから送信されるユーザID及びパスワードを前記会員情報と照合することによってユーザ認証を行うユーザ認証手段を有することを特徴とする。請求項6のネットワーク接続方法は、請求項1の発明を方法の観点から把握したものであって、ネットワークへの接続回線設備を備えた複数のサーバーを用い、前記サーバーは、ユーザに関する会員情報を有する認証側サーバーと、前記認証側サーバーと所定の関係を有する接続側サーバーを含むネットワーク接続システムにおいて、前記接続側サーバーは、ユーザから送信されるユーザID及びパスワードを用いて前記認証側サーバーにユーザ認証を求め、前記ネットワークへの接続を認証の結果に応じてユーザに提供し、前記認証側サーバーは、前記接続側サーバーから送信されるユーザID及びパスワードを前記会員情報と照合することによってユーザ認証を行うことを特徴とする。

【0007】請求項1、6の発明では、ユーザーは、自己の会員情報を保有する認証側サーバーが混雑しているときや、認証側サーバーが地理的に遠い場合、他のサーバーである接続側サーバーにユーザIDとパスワードを送信することによってログイン要求を行う。ユーザが送信したユーザIDとパスワードは、接続側サーバーから認証側サーバーに転送され、認証側サーバーで会員情報と照合することによってユーザ認証が行われる。接続側サーバーでは、ユーザ認証の結果を受けてログイン処理が行われるので、ユーザはインターネット接続サービスを利用することができる。

【0008】請求項2の発明は、請求項1記載のネットワーク接続システムにおいて、前記接続側サーバー及び認証側サーバーはそれぞれ、前記ネットワークへの接続の開始及び終了に関する所定の情報を送受信することによって、接続ログを記録する記録手段を有することを特徴とする。請求項2の発明では、接続側と認証側のサーバー間で情報を送受信することによって、双方同一内容のログを記録するので、ログの信頼性が向上する。

【0009】請求項3の発明は、請求項2記載のネットワーク接続システムにおいて、前記接続側サーバーの前記記録手段及び前記認証側サーバーの前記記録手段は、前記接続の開始から終了に至る間、所定の間隔で所定の情報を送受信することによって前記接続が継続しているか否かを確認するように構成されたことを特徴とする。請求項3の発明では、接続開始から終了まで、接続側と認証側のサーバー間で接続が継続しているか否かの確認が所定の間隔で行われるので、接続ログに記録される内容の信頼性が向上する。

【0010】請求項4の発明は、請求項1、2又は3記載のネットワーク接続システムにおいて、相互に所定の関係を有する複数のサーバーをメンバとして登録する登録手段と、任意のサーバーがメンバであるか否かの問い

合わせに応答するサーバー認証手段と、を有するメンバー登録用サーバーを備えたことを特徴とする。請求項 4 の発明では、複数のサーバーがグループのメンバーとなつて、会員情報及び接続回線設備を相互利用する場合、単一のメンバー登録用サーバーにメンバーの情報が集中する。このため、サーバーごとにメンバーの情報を保有して更新する必要がなくなり、更新ミスやメンバー情報の漏洩が生じにくく、優れたセキュリティが発揮される。

【0011】請求項 5 の発明は、請求項 1, 2, 3 又は 4 記載のネットワーク接続システムにおいて、前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーが、前記ユーザ認証のために授受する情報を暗号化し及び復号するための暗号管理手段を有することを特徴とする。請求項 7 の発明は、請求項 5 の発明を方法の観点から把握したものであって、請求項 6 記載のネットワーク接続方法において、前記接続側サーバーに接続するためのユーザ端末及び前記認証用サーバーは、前記ユーザ認証のために授受する情報を暗号化し及び復号するための処理を実行することを特徴とする。請求項 5, 7 の発明では、パスワードなど、本来は認証側サーバー固有の情報は、暗号化された状態で接続側サーバーを通過する。このため、接続側サーバーや、パスワードが經由するインターネット上のサーバーによってパスワードなどの情報が盗取されることがない。

【0012】請求項 8 の発明は、ネットワークへの接続サービスをユーザ端末から受け付ける接続側サーバーと、ユーザに関する会員情報に基づいてユーザ認証を行う認証側サーバーと、を用いたネットワーク接続方法において、ユーザ端末と認証側サーバーとの間で、ユーザ ID 及びパスワードの授受を、前記接続側サーバーを経由して暗号を用いて行うために、認証側サーバーが、一時的公開鍵 T-Pk を固有の秘密鍵 F-Sk で暗号化することによって第 1 の暗号データを作成するステップと、認証側サーバーが、作成した前記第 1 の暗号データをユーザ端末に送信するステップと、ユーザ端末が、送信された前記第 1 の暗号データから、前記固有の秘密鍵 F-Sk に対応する公開鍵 F-Pk を用いて前記一時的公開鍵 T-Pk を復号するステップと、ユーザ端末が、復号した前記一時的公開鍵 T-Pk を用いて、ユーザ ID 及びパスワードを暗号化することによって第 2 の暗号データを作成するステップと、ユーザ端末が、作成した前記第 2 の暗号データを認証側サーバーに送信するステップと、認証側サーバーが、送信された前記第 2 の暗号データから、前記一時的公開鍵 T-Pk に対応する一時的秘密鍵 T-Sk を用いてユーザ ID 及びパスワードを復号するステップと、を含むことを特徴とする。

【0013】請求項 8 の発明では、認証側サーバーが一時的公開鍵を発行し、ユーザ端末 T から接続側サーバー経由で認証側サーバーへ送信されるユーザ ID 及びパスワードは、一時的公開鍵によって暗号化される。このた

め、ユーザ ID 及びパスワードが接続側サーバーなどの第三者に盗取されることがなく、悪意ある接続側のプロバイダが、ユーザ ID 及びパスワードを利用して接続の事実を偽装するなどの不正が回避できる。

【0014】なお、ユーザ ID 及びパスワードを暗号化する鍵として毎回変更される一時的公開鍵を用いるのは、暗号が經由する接続側サーバーが暗号自体をコピーして保存しておき、暗号を認証側サーバーに再送することによって実在しない接続を偽装し、不正な課金請求を起こすのを防止するためである。また、一時的公開鍵自体を暗号化するのは、端末 T 側で当該暗号を固有の公開鍵で復号することによって、当該一時的公開鍵が確かに認証側サーバーから送信されたものであることを確認できるようにするためである。

【0015】

【発明の実施の形態】次に、本発明の実施の形態（以下「実施形態」という）について、図面にしたがって具体的に説明する。

【0016】（1）第 1 実施形態の構成

第 1 実施形態は、請求項 1～5 に対応するネットワーク接続システム（以下「本システム」という）及びこのネットワーク接続システム上で実行されるネットワーク接続方法（請求項 6, 7 に対応）に関するものである。まず、図 1 は、本システムの概略的構成を示すブロック図である。

【0017】この図に示すように、本システムは、ネットワーク N への接続回線設備を備えた二つのサーバー S1, S2 を有し、サーバー S1 はユーザに関する会員情報 I を有する認証側サーバーになっており、サーバー S2 は、認証側サーバー S1 との提携関係（請求項 1 にいう「所定の関係」）を有する接続側サーバーになっている。認証側サーバー S1 及び接続側サーバー S2 はそれぞれ、通信サーバー C を介してインターネット N に接続され、ユーザ端末 T はモデム M を通じて通信サーバー C にアクセスする。

【0018】認証側サーバー S1 及び接続側サーバー S2 は、それぞれ、ホストプログラム P1, P2 によって制御される。接続側サーバー S2 及び認証側サーバー S1 はそれぞれ、接続の事実を記録するための副ログ S22 及び正ログ S12（請求項 2 にいう接続ログに相当するもの）を備え、副ログ S22 及び正ログ S12 には原則として同一の情報が記録される。

【0019】また、本システムは、相互に提携関係を有するサーバーをメンバーとして登録し、サーバーがメンバーであるか否かの問い合わせに回答するサーバーであるセンタ S3（請求項 4 にいうメンバー登録用サーバーに相当するもの）を備えている。

【0020】図 2 は、本システムの認証側サーバー S1、接続側サーバー S2、ユーザ端末 T 及びセンタ S3 の具体的構成を示す機能ブロック図であり、この図にお

10

20

30

40

50

いて、図 1 に示したインターネット N、通信サーバー C 及び各モデム M は省略する。

【0021】すなわち、接続側サーバー S 2 は、ユーザ端末 T から送信されるユーザ ID 及びパスワードを用いて認証側サーバー S 1 にユーザ認証を求め、認証の結果に応じてユーザ端末 T にインターネット N への接続サービスを提供する接続手段 S 2 1 を有する。一方、認証側サーバー S 1 は、接続側サーバー S 2 から送信されるユーザ ID 及びパスワードを会員情報 I と照合することによってユーザ認証を行うユーザ認証手段 S 1 1 を有する。また、接続側サーバー S 2 及び認証側サーバー S 1 はそれぞれ、接続開始及び接続終了に関する所定の情報を送受信することによって、副ログ S 2 2 及び正ログ S 1 2 を記録する記録手段 S 2 3, S 1 3 を有する。

【0022】本システムを通してインターネットに接続するために、ユーザは、パーソナルコンピュータを所定の接続用プログラムで駆動して成るユーザ端末 T を用いる。このユーザ端末 T と認証側サーバー S 1 は、それぞれ、ユーザ認証のために授受する情報を暗号化し及び復号するための暗号管理手段 T 1 及び S 1 4 を有する。一方、接続用サーバー S 2 は、ユーザから送信された前記暗号を認証用サーバー S 1 に転送するように構成され、認証用サーバー S 1 は、転送された前記暗号からユーザ ID 及びパスワードを復号する暗号管理手段 S 1 4 を有する。

【0023】なお、接続側サーバー S 2 の記録手段 S 2 2 及び認証側サーバー S 1 の記録手段 S 1 2 は、所定の間隔で情報を交換することによってユーザによる接続が継続しているか否かを確認するように構成されている。

【0024】また、センタ S 3 は、相互に所定の関係を有するサーバーをメンバとしてメンバリスト S 3 1 に登録する登録手段 S 3 2 と、サーバーがメンバであるか否かの問い合わせに回答するサーバー認証手段 S 3 3 と、を有する。このセンタ S 3 は、接続側サーバー S 2 と認証側サーバー S 1 との間で情報を交換するために必須なわけではないが、接続側サーバー S 2 及び認証側サーバー S 1 とは別の第三者的主体として、メンバの確認などを行うことによって安全性を高める効果があるので、設置されることが望ましい。各サーバー S 1, S 2, S 3 間の通信は、TCP/IP などのインターネットプロトコル上で行われ、かつ、必要に応じて暗号化が施される。

【0025】(2) 第 1 実施形態の作用及び効果
上記のような構成を有する第 1 実施形態において、インターネット N への接続サービスは、次のような手順で行われる。なお、認証側サーバー S 1 及び接続側サーバー S 2 は、相互に提携関係を有するメンバとして、センタ S 3 のメンバリスト S 3 1 にあらかじめ登録されているものとする。

【0026】(2-1) 事前準備

インターネット接続サービスを利用しようとするユーザは、所望のプロバイダを選択して接続サービスの契約を行う。この場合、本実施形態におけるユーザは、従来と異なり、地理的に遠いプロバイダであっても、自分にとって契約条件などが望ましいプロバイダを自由に選択して契約してよい。ユーザが契約したプロバイダ（加入プロバイダ）のサーバーには、ユーザの会員情報、特にユーザ ID とパスワードが格納され、加入プロバイダ自身のサーバーが、本発明にいう認証側サーバー S 1 となる。ここでは、ユーザ端末 T のユーザに関し、ユーザ ID 及びパスワードを含む会員情報 I が、認証側サーバー S 1 に登録されているものとする。

【0027】加入プロバイダは、自己のサーバーへの接続用電話番号と共に、提携先プロバイダのサーバーへの接続用電話番号をユーザに知らせる。提携先プロバイダのサーバーが本発明にいう接続側サーバー S 2 である。提携は、プロバイダ相互間における 1 対 1 の関係には限定されず、何らかの組織に各プロバイダが加入することによって行うこともでき、この場合、センタ S 3 のメンバリスト S 3 1 に登録されているプロバイダのサーバーが、相互に提携関係を有する正しい接続業者となる。

【0028】(2-2) 接続要求

図 3 は、第 1 実施形態における処理手順を示すフローチャートである。ユーザは、インターネット接続サービスを利用するときは、ユーザ端末 T と電話回線を用いて、サーバーに接続する。接続先となるサーバーは、通常は、加入プロバイダのサーバー S 1 である。しかし、加入プロバイダのサーバー S 1 の接続回線が混雑しているために電話がつかない場合や、ユーザにとって加入プロバイダのサーバー S 1 が遠隔の場合、ユーザは、前記提携先プロバイダのサーバー S 2 に接続要求を行う（ステップ 301）。

【0029】なお、ユーザ端末 T は、専用の接続手順によって動作する。すなわち、接続要求にはユーザ ID 及びパスワードを送信するが、加入プロバイダ以外のプロバイダに接続要求する場合は、ユーザ端末 T の暗号管理手段 T 1 が、ユーザ ID 及びパスワードを暗号化して接続側サーバー S 2 に送信する。なお、ユーザ ID 及びパスワードを暗号化する場合でも、接続側サーバー S 2 で認証側サーバー S 1 を特定できるように、ユーザ端末 T は、暗号化されたユーザ ID 及びパスワードに、認証側のプロバイダ又はサーバーを示す識別子を付加して接続側サーバー S 2 に送信する。また、識別子の付加に代えて、ユーザ ID のうち、認証側サーバー S 1 を特定する表示の部分は暗号化せずに接続側サーバー S 2 に送信するようにしてもよい。例えば、ユーザ ID の形式が "xxx @aaa.or.jp" の場合、"xxx" の部分は暗号化し、"@aaa.or.jp" の部分は暗号化せずに送信する。

【0030】(2-3) サーバー認証

ユーザから接続要求を受けた接続側サーバー S 2 では、

接続手段 S 2 1 が接続要求を受け付ける。接続手段 S 2 1 は、接続要求に係るユーザ ID の形式が他のサーバーのもの（例えば“xxx@aaa.or.jp”）である場合、当該他のサーバー S 1 (aaa.or.jp) がメンバであるか否かをセンタ S 3 に問い合わせる（ステップ 3 0 2）。問い合わせを受けたセンタ S 3 では、サーバー認証手段 S 3 3 が、メンバリスト S 3 1 との照合によって、問い合わせに係る認証側サーバー S 1 がメンバであるか否かを確認し、問い合わせに回答する。

【0031】（2-4）ユーザ認証

ユーザ ID に係るサーバー S 1 がメンバであることが確認されると、接続側サーバー S 2 の接続手段 S 2 1 は、接続要求に係る認証側サーバー S 1 にユーザ ID 及び暗号化されているパスワードを転送することによって、ユーザ認証（ユーザ ID 及びパスワードが真正なものであるか否かを確認すること）を求める（ステップ 3 0 3）。

【0032】このとき、ユーザ認証を要求された認証側サーバー S 1 でも、認証要求を発行した接続側サーバー S 2 がメンバであるか否かをセンタ S 3 に照会して確認する。問い合わせを受けたセンタ S 3 は、メンバリスト S 3 1 と照合することによって、問い合わせに係る接続側サーバー S 2 がメンバであるか否かを確認し、問い合わせに回答する。問い合わせに係る接続側サーバー S 2 がメンバであることが確認されると、認証側サーバー S 1 の暗号管理手段 S 1 4 が、暗号からパスワードを復号する。

【0033】そして、ユーザ認証手段 S 1 1 が、転送されてきたユーザ ID 及び復号されたパスワードを会員情報 I と照合し、真正なユーザ ID 及びパスワードであるか否かを確認することによってユーザ認証を行い、その結果を接続側サーバー S 2 に返信する。なお、サーバー認証やユーザ認証において、サーバーがメンバでなかったり、パスワードの不一致などで、否定的な結果となったときは、接続は当然に拒絶される。

【0034】（2-5）接続開始と記録

返信されてきた認証結果が応諾（肯定的）ならば、接続側サーバー S 2 の接続手段 S 2 1 は、ユーザ端末 T との間で PPP 接続を開始する（ステップ 3 0 4）と共に、記録手段 S 2 3 が認証側サーバー S 1 に接続開始通知を送信する（ステップ 3 0 5）。認証側サーバー S 1 の記録手段 S 1 3 は、接続開始通知を受信すると、正ログ S 1 2 にユーザ ID 及び開始時刻を記録する（ステップ 3 0 6）と共に、接続開始受諾通知を接続側サーバー S 2 に送信する（ステップ 3 0 7）。接続側サーバー S 2 の記録手段 S 2 3 は、接続開始受諾通知を受信すると、認証側サーバー S 1 の正ログ S 1 2 と同様に、ユーザ ID 及び開始時刻を副ログ S 2 2 に記録する（ステップ 3 0 8）。

【0035】（2-6）接続の監視

その後、接続側サーバー S 2 における接続が終了し（ステップ 3 1 0）、接続側サーバー S 2 から認証側サーバー S 1 に接続終了通知が送信されるまで、認証側サーバー S 1 は、接続が継続していることを一定間隔で接続側サーバー S 2 に確認することによって（ステップ 3 0 9）、接続を監視する。

【0036】（2-7）接続の終了

ユーザが所定の接続終了操作を行うと（ステップ 3 1 0）、接続側サーバー S 2 の接続手段 S 2 1 がユーザ端末 T との間で PPP 接続を終了すると共に、記録手段 S 2 3 が認証側サーバー S 1 に接続終了通知を送信する（ステップ 3 1 1）。認証側サーバー S 1 の記録手段 S 1 3 は、接続終了通知を受信すると、正ログ S 1 2 に接続終了の旨及び終了時刻を記録すると共に、接続終了確認通知を接続側サーバー S 2 に送信する。接続側サーバー S 2 の記録手段 S 2 3 は、接続終了確認通知を受信すると、認証側サーバー S 1 の正ログ S 1 2 と同様に、ユーザ ID 及び終了時刻を副ログ S 2 2 に記録する。

【0037】（2-8）課金の精算

20 認証側サーバー S 1 の正ログ S 1 2 及び接続側サーバー S 2 の副ログ S 2 2 は所定の期日に突合（照合）され、一致した接続に関して課金が精算される。

【0038】（2-9）第 1 実施形態による効果

以上説明したように、第 1 実施形態によれば、ユーザーは、自己の会員情報を保有する認証側サーバーが混雑しているときや、認証側サーバーが地理的に遠い場合、他のサーバーである接続側サーバーにユーザ ID とパスワードを送信することによって接続要求を行う。ユーザが送信したユーザ ID とパスワードは、接続側サーバーから認証側サーバーに転送され、認証側サーバーで会員情報と照合することによってユーザ認証が行われる。接続側サーバーでは、ユーザ認証の結果を受けてユーザにインターネット接続サービスを提供する。

【0039】これによって、混雑時でもネットワークへのつながりやすさ（接続可能性）が改善される。また、ユーザは遠隔のプロバイダとも契約できるので、プロバイダの会員募集の対象地域が拡大する。また、プロバイダは、独自に会員募集を行わず、接続側サーバーのみを提供することもできるので、プロバイダ経営が多様化する。第 1 実施形態によれば上記のような効果を通じて、インターネットの健全な普及が実現される。

【0040】また、第 1 実施形態では、接続要求の際のパスワードなどの情報は、暗号化された状態でユーザから接続側サーバーを通過し認証側サーバーに到達する。このため、接続側サーバーのプロバイダによるパスワードなどの盗取が防止される。

【0041】また、第 1 実施形態では、複数のサーバーがグループのメンバとなって、会員情報及び接続回線設備を相互利用する場合、単一のセンタにメンバの情報を蓄積しておくことができる。そして、接続側サーバー及

10

20

30

40

50

び認証側サーバーのいずれも、ユーザの接続要求に係る相手方がメンバか否かをセンタに問い合わせることによって確認できる。このため、メンバから脱退したプロバイダやメンバ以外のプロバイダなど、無権限な第三者が接続側サーバーのプロバイダになりすますことによって、接続サービスの課金請求を起こすことを回避できる。また、メンバーの情報は単一のセンタに蓄積される。このため、サーバーごとにメンバの情報を保有して更新する必要がなくなり、更新ミスやメンバ情報の漏洩が生じにくく、優れたセキュリティが発揮される。

【0042】また、第1実施形態によれば、接続側と認証側のサーバー間で情報を送受信することによって、双方同一内容のログを記録するので、いずれかのサーバーによるログの偽造も防止され、ログの信頼性が向上する。

【0043】また、第1実施形態によれば、接続開始から終了まで、接続側と認証側のサーバー間で接続が継続しているか否かの確認が所定の間隔で行われるので、接続ログに記録される内容の信頼性が向上する。

【0044】(3) 第2実施形態

前記第1実施形態においてもパスワード等を暗号化及び復号したが、パスワード等の暗号化に用いる鍵を毎回変更することによって、よりセキュリティ性を改善することができる。また、接続側サーバーS2と認証側サーバーS1との間で接続開始を通知したりログに記録する手順も第1実施形態に示したとおりである必要はない。第2実施形態は、第1実施形態と同様の構成を有するネットワーク接続システムにおいて、パスワード等の暗号化に用いる鍵を毎回変更することによって、よりセキュリティ性を改善した例であり(請求項8に対応)、また、

【0045】(3-1) ユーザ認証までの手順

図4は、第2実施形態における接続要求からユーザ認証までの処理手順を示すフローチャートである。すなわち、まず、ユーザ端末Tから接続側サーバーS2に接続要求があると(ステップ401)、接続側サーバーS2の接続手段S21が、接続要求に係る認証側サーバーS1がメンバであることを、センタS3によるサーバー認証を求めて確認したうえ(ステップ402)、接続側サーバーS2から認証側サーバーS1へ新たな接続要求があったことを通知する(ステップ403)。

【0046】接続要求の通知を受けた認証側サーバーS1のユーザ認証手段S11でも、接続要求に係る接続側サーバーS2がメンバであることを、センタS3によるサーバー認証を求めて確認する(ステップ404)。なお、以下の説明で用いる暗号鍵は公開鍵暗号方式PGPを前提とし、毎回変更される

一時的公開鍵T-Pk (暗号化用)

一時的秘密鍵T-Sk (復号用)

のペア及び固定された

固有の秘密鍵F-Sk (暗号化用)

固有の公開鍵F-Pk (復号用)

のペアを用いる。

【0047】すなわち、接続側サーバーS2がメンバであることをサーバー認証で確認した認証側サーバーS1の暗号管理手段S14は、一時的公開鍵T-Pkを決定し、固有の秘密鍵F-Skで一時的公開鍵T-Pkを暗号化することによって第1の暗号データを作成する(ステップ405)。一時的公開鍵T-Pkは、端末Tから認証側サーバーS1へ、ユーザ認証のためのユーザID及びパスワードを暗号化して送信するためのものである。

【0048】ここで、固有の秘密鍵F-Skは固定されたものであるが、一時的公開鍵T-Pkは毎回変更される。認証側サーバーS1のユーザ認証手段S11は、作成した前記第1の暗号データを、接続側サーバーS2を経由して端末Tに送信する(ステップ406)。端末Tには、固有の秘密鍵F-Skに対応する固有の公開鍵F-Pkがあらかじめ与えられており、端末Tの暗号管理手段T1は、送信された前記第1の暗号データから、固有の公開鍵F-Pkを用いて前記一時的公開鍵T-Pkを復号する(ステップ407)。

【0049】続いて、端末Tの暗号管理手段T1は、復号した前記一時的公開鍵T-Pkを用いて、ユーザID及びパスワードを暗号化することによって第2の暗号データを作成し(ステップ408)、作成した前記第2の暗号データを、接続側サーバーS2を経由して認証側サーバーS1に送信する(ステップ409)。第2の暗号データを受信した認証側サーバーS1の暗号管理手段S14は、送信された第2の暗号データから、前記一時的公開鍵T-Pkに対応する一時的秘密鍵T-Skを用いてユーザID及びパスワードを復号する(ステップ410)。そして、認証側サーバーS1のユーザ認証手段S11が、復号したユーザID及びパスワードを自己の会員情報Iと照合して真正なものであるか否かを確認することによってユーザ認証を行い(ステップ411)、その結果を接続側サーバーS2に通知する(ステップ412)。

【0050】第2実施形態では、上記のように、認証側サーバーS1が一時的公開鍵T-Pkを発行し、ユーザ端末Tから接続側サーバーS2経由で認証側サーバーS1へ送信されるユーザID及びパスワードは、一時的公開鍵T-Pkによって暗号化される。このため、ユーザID及びパスワードが接続側サーバーS2などの第三者に盗取されることがなく、悪意ある接続側のプロバイダが、ユーザID及びパスワードを利用して接続の事実を偽装するなどの不正が回避できる。

【0051】なお、ユーザID及びパスワードを暗号化する鍵として毎回変更される一時的公開鍵T-Pkを用いるのは、暗号が経由する接続側サーバーS2が暗号自体をコピーして保存しておき、暗号を認証側サーバーS1に再送することによって実在しない接続を偽装し、不正な課金請求を起こすのを防止するためである。また、一時的公開鍵T-Pk自体を暗号化するのは、端末T側で当該暗号を固有の公開鍵F-Pkで復号することによって、当該一時的公開鍵T-Pkが確かに認証側サーバーS1から送信されたものであることを確認できるようにするためである。

【0052】(3-2) ユーザ認証以降の手順

図5は、第2実施形態において、ユーザ認証以降の手順を示すフローチャートである。すなわち、正しいユーザID及びパスワードによってユーザ認証が無事に終了すると、認証側サーバーS1の記録手段S13は、センタS3及び接続側サーバーS2に、接続許諾通知と接続の開始時刻を通知するとともに、その旨と開始時刻を正ログS12に記録する(ステップ501)。接続側サーバーS2では、この通知を受け、接続手段S21がユーザ端末Tとの間でPPP接続を開始すると同時に、記録手段S23が接続開始時刻を副ログS22に記録する(ステップ502)。なお、センタS3及び接続側サーバーS2は、接続許諾通知を受信した場合、受信確認を認証側サーバーS1へ送信する(ステップ503)。

【0053】接続開始後は、接続側サーバーS2及び認証側サーバーS1は、接続終了まで、それぞれ一定間隔で他方に対して接続が継続していることを確認する。すなわち、接続側サーバーS2の記録手段S23は、ユーザによる接続終了操作が行われたり回線切断による自動ログアウトが発生するまで、認証側サーバーS1の記録手段S13に対して一定間隔で、接続の継続を表すデータを送信する。そして、接続側サーバーS2の記録手段S23は、この送信に対して確認のための返信を認証側サーバーS1の記録手段S13から受けることによって、認証側サーバーS1が接続の継続を認識していることを確認する(ステップ505)。

【0054】一方、認証側サーバーS1の記録手段S13は、接続側サーバーS2から接続終了の通知を受け取るまで、接続側サーバーS2の接続手段S21に対して一定間隔で、接続の継続を問い合わせるデータを送信する。そして、認証側サーバーS1の記録手段S13は、この送信に対する返信を接続側サーバーS2の接続手段S21から受信することによって、接続側サーバーS2における接続が継続していることを確認する(ステップ506)。

【0055】接続側サーバーS2の記録手段S23は、ユーザの端末Tから接続終了を表す信号を受け取った場合(ステップ504)、認証側サーバーS1及びセンタS3に接続終了通知と接続終了時刻を送信する(ステッ

507)。認証側サーバーS1の記録手段S13は、接続終了通知及び接続終了時刻を受信した場合、正ログS12に接続終了の旨及び接続終了時刻を記録すると共に(ステップ508)、接続側サーバーS2及びセンタS3へ接続終了確認通知を送信する(ステップ509)。この接続終了確認通知を受信した接続側サーバーS2の記録手段S23は、副ログS22に接続終了の旨及び接続終了時刻を記録する。

【0056】なお、接続の開始や終了は、接続側サーバーS2及び認証側サーバーS1からの通知を受けて、センタS3でも所定のログ(図示せず)に記録される。そして、認証側サーバーS1及び接続側サーバーS2の正ログS12及び副ログS22は、所定の期日にセンタS3へ送られ、センタS3のログを含む計3つのログが相互に突合され、一致しているデータが課金請求などの処理へ回される。

【0057】第2実施形態では、上記のように、接続開始通知や接続開始時刻など接続に関する情報がセンタS3にも送信され、センタS3でも正ログS12や副ログS13と同様の記録が行われるので、ログの正確性と信頼性が一層向上する。

【0058】また、第2実施形態では、接続継続の確認は、認証側から接続側及び接続側から認証側へという双方向で行われる。これによって、まず、接続側サーバーS2がダウンしたり、又は障害のために認証側に終了通知を送信できない場合も、認証側からの確認によって接続の終了が判明するので、認証側サーバーS1は、接続の終了を正しく接続ログに記録することができる。また、認証側サーバーS1がダウンしたり、又は障害のために接続側からの終了通知を認識できない場合も、接続側サーバーS2は確認によってそれらの事態を把握し、例外処理を起動するなど必要な処理を行うことができる。

【0059】(4) 他の実施形態

なお、本発明は上記実施の形態に限定されるものではないので、次に例示するような他の実施の形態をも包含するものである。例えば、接続側サーバーと認証側サーバーという種別はユーザとの関係で定まる相対的なもので、具体例を挙げれば、図2の接続側サーバーS2が独自に会員と会員情報を持っていたとしても差しつかえない。すなわち、認証側サーバーは、接続要求に係るユーザの会員情報を保有しているサーバーを意味し、サーバーS2のプロバイダと契約しているユーザがサーバーS1に接続要求する場合は、ユーザにとっては、前記各実施形態とは逆に、サーバーS1が接続側サーバーとなり、サーバーS2が認証側サーバーとなる。

【0060】また、メンバー登録用サーバーであるセンタS3は必ずしも設ける必要はなく、認証側サーバー及びユーザ端末の暗号管理手段を設けずに本発明を実施することも技術的には可能である。また、本発明は、インタ

ーネットへの接続のみならず、他の広域ネットワークへの接続にも適用することができる。

【0061】

【発明の効果】以上説明したように、本発明によれば、複数のサーバー間で会員情報及び接続回線設備を相互利用できるので、接続性に優れたネットワーク接続システム及びネットワーク接続方法を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態の概略的構成を示すブロック図

【図2】本発明の第1実施形態の要部の構成を示す機能ブロック図

【図3】本発明の第1実施形態における処理手順を示すフローチャート

【図4】本発明の第2実施形態におけるユーザ認証までの処理手順を示すフローチャート

【図5】本発明の第1実施形態におけるユーザ認証以降の処理手順を示すフローチャート

【符号の説明】

S 1 …認証側サーバー

S 1 1 …ユーザ認証手段

S 1 2 …正ログ

S 1 3 …記録手段

S 1 4 …暗号管理手段

S 2 …接続側サーバー

S 2 1 …接続手段

S 2 2 …副ログ

S 2 3 …記録手段

S 3 …センタ（メンバ登録用サーバー）

10 S 3 1 …メンバリスト

S 3 2 …登録手段

S 3 3 …サーバー認証手段

C …コミュニケーションサーバー

I …会員情報

M …モデム

N …インターネット

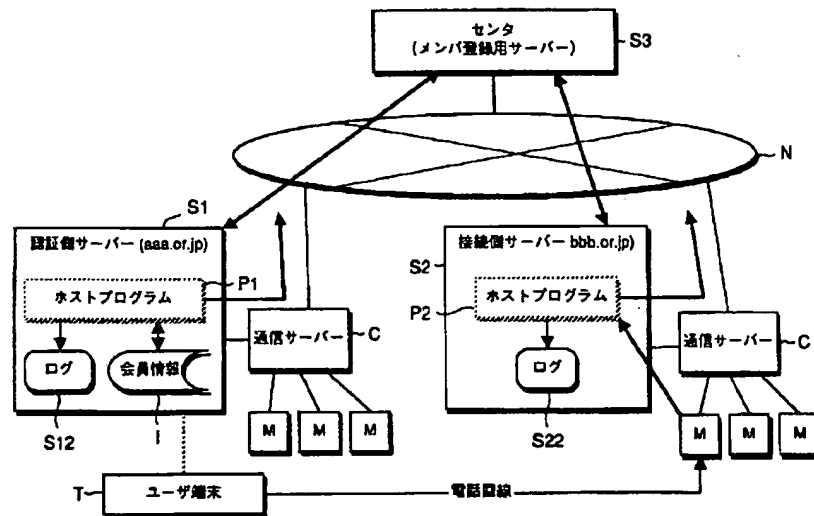
P 1, P 2 …ホストプログラム

STEP …手順の各ステップ

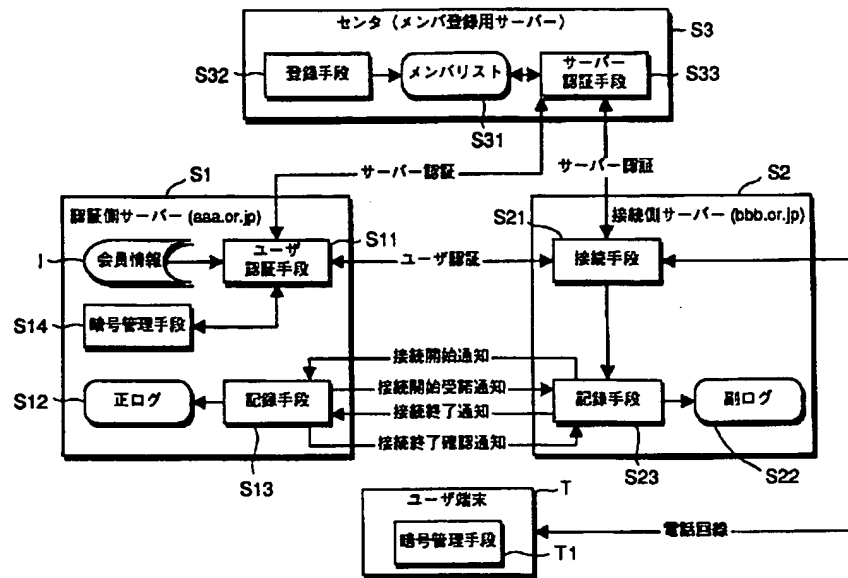
T …ユーザ端末

20 T 1 …暗号管理手段

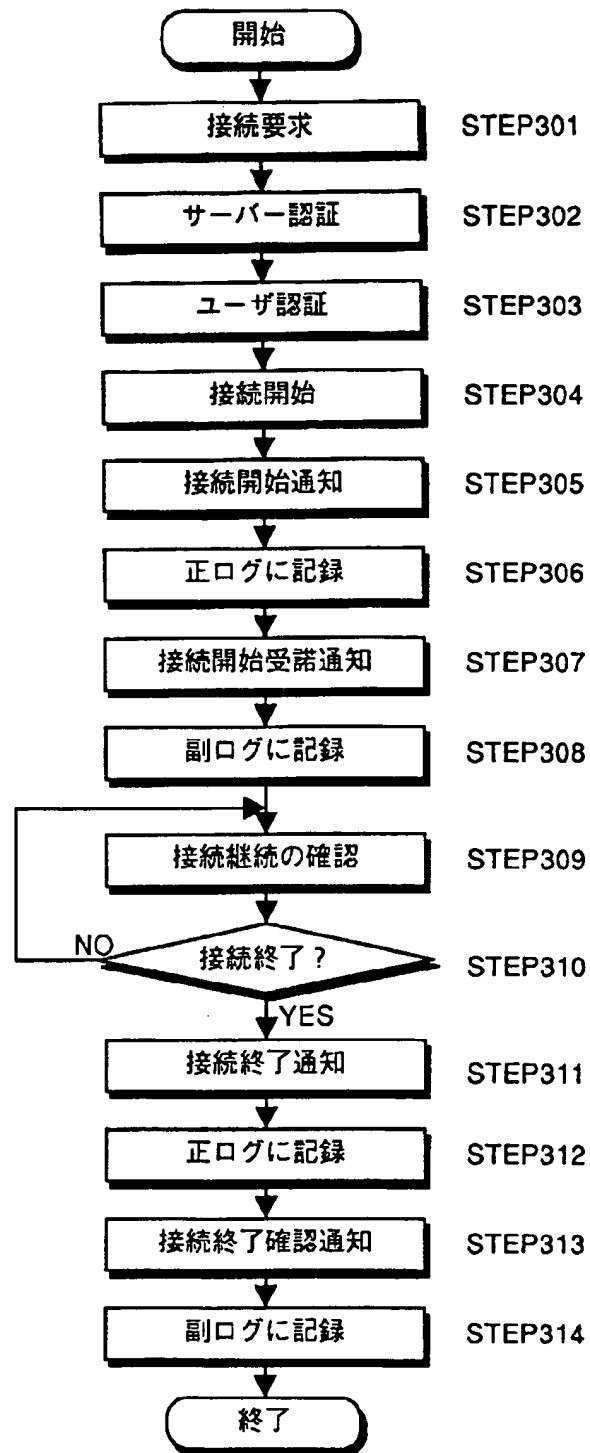
【図1】



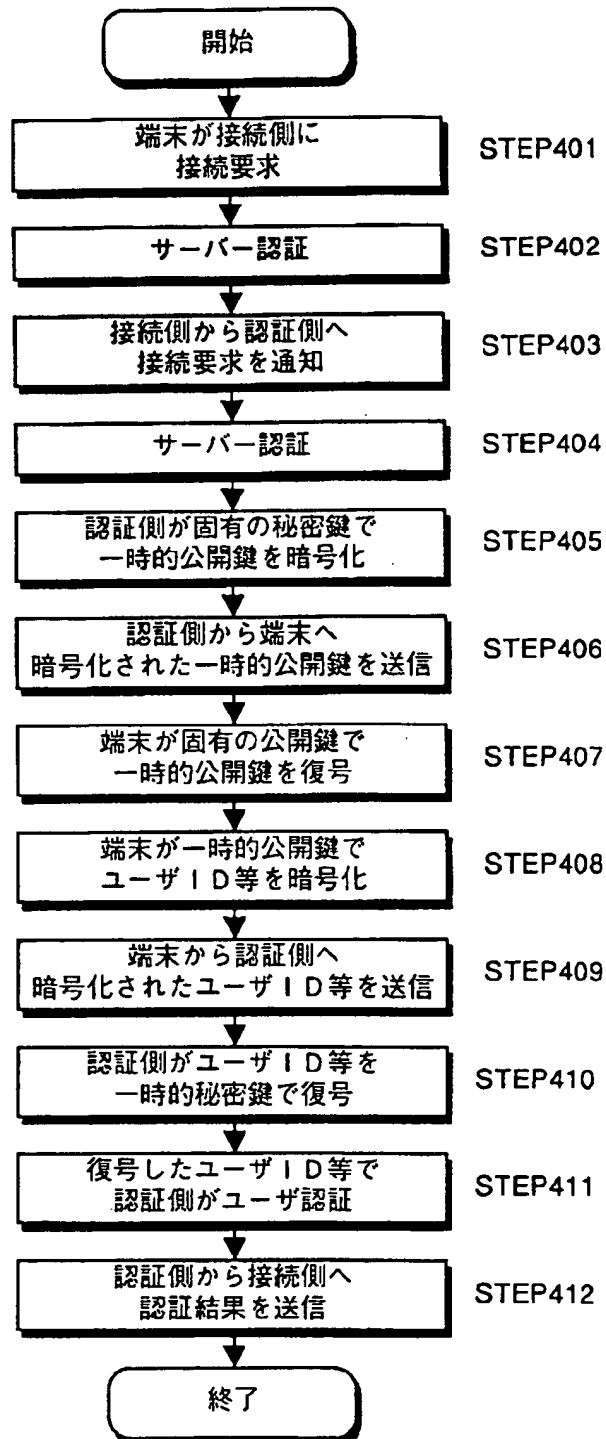
【図 2】



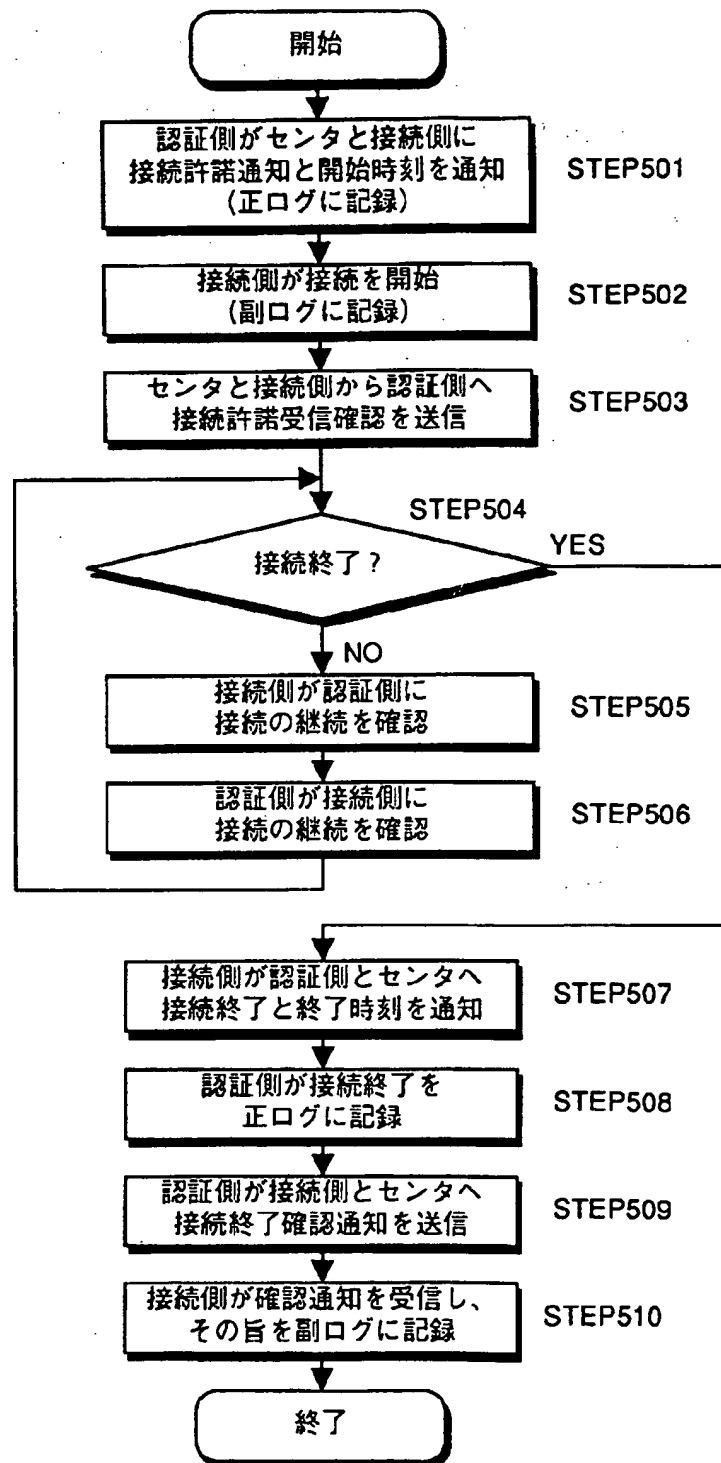
【図 3】



【図 4】



【図 5】



フロントページの続き

(51) Int. Cl. ⁶

識別記号

F I

673

A

(72) 発明者 山本 敏淳

北海道札幌市中央区南 2 条西 7 丁目 6-2

日宝南 2 条ビル 5 階 株式会社アド・ホ
ック内